Combatting Cyber Extremism in the Global Environment

By Dr. Lynne Manganaro

Editorial Abstract: Dr. Manganaro analyzes terrorist use of the Internet, examining extremist goals, methods and tactics. She addresses current shortfalls in Department of Defense efforts to counter these actions, and recommends use of existing doctrinal guidance to enhance the US counter-cyber campaign.

"... How it is that a nation that gave rise to Silicon Valley, Hollywood, and Madison Avenue came to be outplayed in the realm of ideas, effectively communicated in the new media?"

-- Homeland Security Institute

The information environment poses a unique challenge to Department of Defense (DOD) efforts to neutralize Al Qaeda and other extremist Islamist organizations. Communication mediums such as television, radio, newspapers, and the Internet facilitate the world-wide reach and flow of extremist ideology. But only the Internet possesses unfettered access to, and maneuverability through, the global information environment, whereas other mediums face limitations in terms of broadcast range and cost with respect to production and delivery. Moreover, unconstrained by national or political boundaries, information passed via the Internet can reach global audiences in the blink of an eye. These are just some of the characteristics of the information environment that challenge DOD efforts to combat the spread of extremist messaging.

Extremist groups, particularly AQ, understand the Internet's power. AQ uses the Internet in two primary ways: as a command and control (C2) network, and as a dissemination mechanism. A recent report by the Homeland Security Policy Institute notes the Internet has made many terrorist operational activities cheaper, faster, and more secure. Unlike more traditional communication mediums, the Internet offers a wide-range of multi-media functionality such as text, two-dimensional images, music, and videos. To date, the bulk of GWOT efforts center on degrading AQ's use of the Internet as a C2 network through direct action (kinetic operations) and technological solutions (which fall into the realm of Computer Network Operations). DOD directs less effort against countering AQ's second, more insidious, use of the Internet—as a dissemination mechanism—to spread extremist ideology and propaganda. Preventing information flow through technological solutions is limited, but Psychological Operations (PSYOP) provide an effective alternative to counter the spread of extremist messaging.

AQ's information propagation is well documented in open sources, and a simple *Google* search using "Al Qaeda use of Internet" illustrates this. As-Sabah, AQ's media cell, is the primary method of communicating extremist ideological and propaganda messages to current members and potential recruits. This highly sophisticated and independent organization leverages Internet technology for maximum effect. A recent series published by *The Global Issues Reports* provide a disturbing examination into the efficiency and effectiveness of As-Sabah.

The series chronicles the use of charismatic speakers such as Abu Yahya al-Libi and Adam Gadan, and their mass appeal to those engaged in terrorist activities, as well as potential recruits. Abu Yahya captured the spotlight with his widely publicized escape from US custody in Bagram, Afghanistan in July 2005. Adam Gadan's appeal stems from his being a white middle-class California convert to Islam. The celebrity surrounding these two individuals, coupled with the professional production capabilities of As-Sabah; generate highly sophisticated multi-media products that resonate with target audiences of young Muslim males. Once products are released, distribution is unlimited, particularly when downloaded, emailed, and transferred to other media forms. In addition, AQ members and potential recruits turn to the Internet for sources of instruction and inspiration. Extremist websites offer a variety of instructional materials such as weapons training, bomb-making, and tactics as well as footage of beheadings and video letters left behind by suicide bombers. Streaming video feeds on cell phones, add another real time dimension to the reach and effectiveness of extremist messaging.

AQ's embrace of the Internet appears contradictory, given their stated desire to re-establish the 7th century Caliphate. Their inability to subordinate any nation-state to date perhaps motivated their use of the Internet, to engage in what has been commonly called "cyber-terrorism" or "cyber-extremism." From AQ's perspective, this struggle would lead to a "cyber-caliphate"—a virtual nation in the cyber world. Consequently, shifting from the physical world to the information environment challenges a conventional military structure designed to fight on land, air, sea, and space within demarcated geographic areas.

GWOT falls short in countering extremist messaging on the Internet due to its primary focus on countering the C2 network. Countering extremist messaging can best be addressed by PSYOP. Tim Thomas, a senior analyst in the Foreign Military Studies Office at Ft. Leavenworth, proposes a new term for PSYOP and argues that cyber psychological operations (CYOP) represent a logical extension of its traditional mission—countering enemy propaganda—in the digital age [*IO Sphere* Winter 2007]. The Internet merely represents another communication medium for CYOP to use.

DOD is behind the power curve in addressing the extremist messaging threat. Operating effectively in the information environment requires a concerted effort, because the long-term threat of extremist Internet messaging is unrecognized and therefore unchallenged. Currently, the advantage in the digital information environment belongs to AQ and other extremist organizations that have risen in the past few years.

CNO versus CYOP

A major stumbling block to executing CYOP involves misperceptions regarding the Internet, the biggest of which is the belief that any activity involving the Internet falls in the purview of CNO. However, this perception fails to recognize the Internet as a means to an end (an information conduit), in addition to an end in itself (physical aspect in the form of hardware). While this skewed view of the Internet dominates and defines the issue, doctrine very clearly states CNO and PSYOP roles and responsibilities. According to Joint doctrine, CNO is divided into three general areas: computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE).

From a doctrinal perspective, CND is purely defensive, ensuring protection of DOD computer systems and networks from unauthorized intrusions. CNE is primarily an intelligence collection activity. The one-sided view of CNO dominance over the Internet emerges from a misinterpretation of what constitutes CNA. By definition, CNA is responsible for "disrupting, denying, degrading, or destroying *information* resident in computers and so on" [emphasis added]. From the C2 perspective, this technology-based solution is appropriate. However, when dealing with AQ's use of the Internet as a dissemination mechanism, *"information"* represents an abstract ideology designed to *influence* an audience.

A technology dependent strategy is not an effective long-term solution for countering ideology, for several reasons. First, technology alone cannot prevent extremist messaging from reaching the Internet. Attacking extremist websites is unrealistic, more akin to playing "whack a mole" when these sites reappear. Moreover, anyone with an Internet connection can randomly upload products on sites that are not ordinarily categorized as extremist, hence are not monitored. Second, a technology dependent strategy cannot counter the volume of extant messaging that perpetuates a view of the West, and incites young Muslims to violence. Lastly, technology dependent strategies do not address the *influence* component of the information. In other words, nothing in doctrine suggests CNA is situated to engage in a "war of ideas." Consequently, an effective long-term strategy involves disrupting, denying, degrading, or destroying information (either C2 or extremist messaging), as well as recognizing the influence component of information—which is a PSYOP mission.

Narrow interpretations of CNA's duties and responsibilities limit PSYOP access to the Internet. However, an examination of doctrine reveals no inherent prohibitions against this. Rather, joint doctrine grants PSYOP the ability to use any communication medium for mission accomplishment, as follows:

PSYOP are a vital part of the broad range of US activities to influence foreign audiences and are the only DOD operations authorized to ***influence*** *foreign TAs (target audiences) directly through the use of radio, print, and* ***other media*** [emphasis added].

Thus, doctrine establishes PSYOP primacy as the only DOD component with the authority to influence attitudes or behaviors of designated target audiences. Further, it authorizes PSYOP to use any communication means necessary for mission accomplishment.

Another justification for CNO control relates to the CNE function of intelligence collection. But this is a narrow view of the information environment, and limits our national response to counter cyber-terrorism—and again discounts the influence component of extremist messaging. Doctrine clearly separates the collection requirement of CNE from the influence mission of PSYOP. We should approach these two distinct problems sets in kind.

Another common misperception guiding policy makers is the belief that, given the nature of the Internet, Americans would become targets of PSYOP efforts. These concerns are unfounded. PSYOP programs are methodically researched, by subject matter experts who focus on, and influence, specific target audiences. The effort that goes into product development is similar in scope to the expertise applied to marketing consumer products. Commercial advertisements also target specific audiences, and are designed to elicit a response from those selected targets. Consequently, there is a decreased probability an advertisement would trigger a response in individuals outside the intended target audience. Moreover, the resulting PSYOP products are subject to an approval process that ensures cultural appropriateness of language, content, and symbolism. Since PSYOP targets foreign audiences, products are not produced in English. The probability that Americans, as a group, would be exposed is minimal.

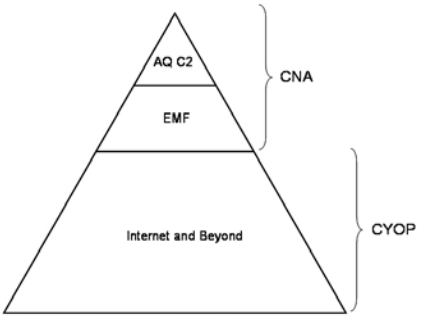

Figure 1. CNO & CYOP levels of responsibility. (Author)

Re-examination of doctrine coupled with questioning common perceptions establishes a new perspective on combating cyber-terrorism. Logic suggests CYOP is the natural evolution of the counter-propaganda and influence mission onto the digital battlefield. Figure 1 delineates the areas of responsibility between CNO and CYOP by level of dissemination. The top level represents the small cadre of AQ's C2 net, the core of its communications architecture. The second level is comprised of what is commonly referred to as the "extremist media forums" (EMF). These are select password protected extremist sites and the recipients of new propaganda releases. For example, the sporadic Zawahiri and Bin Laden videos premiere on these sites. They represent primary distribution points for AQ and other extremist organizations.

Once uploaded to the EMF, registered users can download the products, make hard copies, send through the e-mail, or repost them at the third level. This comprises the larger domain of non-

password protected "pseudo-extremist" sites, including generic non-password protected sites. These range from blogs to popular video sharing and social networking sites, such as *YouTube*, *MySpace*, and *Facebook*.

"It is as if you would watch a Hollywood movie," said Abu Saleh, a 21-year old German devotee of Al Qaeda videos who visits Internet cafes in Berlin twice a week, "The Internet has totally changed my view on things."

Current Policy

DOD efforts to counter extremist Internet messaging consists of an eclectic assortment of authorities, offering no comprehensive strategy in addressing the problem. Current authorities limit activity to geographic regions or a specific countries, with some requiring Department of State approval. However, because the Internet is a subset of the information environment, cyber-extremism should be addressed holistically, rather than in smaller parts. Bin Laden and Zawahiris' videos appeal to global audiences rather than any one geographic region. Therefore, approaching cyber-terrorism from the perspective of recognized national boundaries is problematic.

Dividing the world into neat geographic areas challenges effective policy response by failing to recognize that neither information nor many populace groups distinguish between national or political boundaries. As such, the decentralized nature of cyber-extremism renders the spread of radical Islamist ideology potentially more debilitating to global stability than the old traditional state-sponsored terrorism model. This new ideological threat is trans-national, emanating from no single country. Although GWOT is billed as a global, direct kinetic operations by both conventional and special operations forces have been hamstrung by a military conditioned to wage war against nation-states—and all the legal restrictions this implies.

US military operations also depend upon the goodwill and cooperation of other nations to stage and forward project our military power. When the US attacked Afghanistan after the tragic events of 9/11, we operated under the premise that the Taliban represented the "legitimate" government of Afghanistan, yet at the time only Pakistan, Saudi Arabia, and the United Arab Emirates granted it formal diplomatic recognition. While ideology moves quickly and effortlessly across national and political boundaries, troops cannot. US forces face legal limitations in taking direct military action against AQ elements residing in Pakistan, and or whereever AQ takes refuge.

The Digital Threat

DOD policy is slow to respond to cyber-terrorism, and currently focuses primarily on killing or capturing AQ and other associated terrorists. A kinetic strategy is not an effective long-term solution for dealing with an ideological threat. First, it ignores the move to cyber-terrorism and the establishment of the cyber-caliphate. AQ's failure to gain a foothold in either Afghanistan or Iraq led AQ to recognize the futility of engaging in direct combat actions against a superior, well-trained and equipped military force. Consequently, the vision of subordinating nation states through conquest has been replaced by the more pragmatic approach of establishing a cyber-caliphate. Author Oliver Steeds reports "since 9/11 Al Qaeda's greatest expansion has been through the Internet using affiliated sites like *Al-Ansar, Al-Neda,* and *Al-Islah* for propaganda, education, and communications. Websites, bulletin-boards and chat rooms are the domain of this new 'cyber-caliphate' where the political messages of global extremism are being spread."

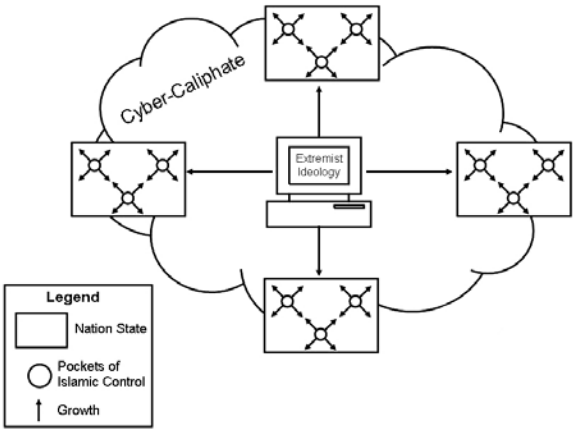

Figure 2. Development of the Cyber-Caliphate. (Author)

Second, each terrorist death exponentially increases the animosity of those pre-disposed toward a radicalized version of Islam. These "martyrs" live on in flashy media products glorifying their deaths with an Islamist version of an alternative reality. More importantly, they function as a radicalization tool—shaping the perceptions and influencing the beliefs of young recruits. A recent US Congressional report states "Islamic insurgency groups have replaced the mosque and seminary with the Internet in efforts to recruit and indoctrinate."

But the idea of a cyber-caliphate would be of little utility if it did not somehow manifest itself in the physical world. Since the odds of a top-down subordination of nation-states under total control of the Caliph are negligible, one can hypothesize that these manifestations would be small pockets of Islamist control. Figure 2 illustrates the development of the cyber-caliphate. Boxes represent nation-states, circles represent the pockets of extremist Islamist control, and arrows represent expansion of these pockets. The Internet is the glue that binds these disparate communities together, connecting them with a common ideology in a virtual community, and diminishing any sense of isolation based on geographic location.

At the macro-level, the model operates like a cancer, invading a healthy organism and establishing itself in one part of the system. At the micro-level, some organisms are less resistant, hence more susceptible to the threat than others. Likewise, some nation-states are more susceptible to the emergence of these pockets. For example, countries with large Muslim populations; fragile political structures, high levels of illiteracy; and under-developed security forces are a few of the conditions facilitating such development. These

pockets can also develop in Western countries where large Muslim enclaves exist, particularly when basic needs are met by the Muslim community and interaction with the larger non-Muslim population is limited or absent.

There is evidence suggesting the genesis of these pockets in two pre-dominantly Muslim countries. First, parts of Somalia are under the control of Islamists spearheaded by the fundamentalist Islamic Courts Union. Many of the war-weary populations welcome the perceived stability they offer. Second, the Federally Administered Tribal Areas (FATA) of Pakistan's North-West Frontier Province (NWFP), an area only nominally controlled by the central government, have long identified as Islamist. Both AQ and the Taliban enjoy freedom of movement and sanctuary in the FATA. Dilapidated, underdeveloped infrastructure notwithstanding, the Internet overcomes time and distance to provide a virtual connection between the two countries. As a result, Internet-enabled extremists can influence the youth in these two areas.

Third, dissemination via the Internet is difficult to combat due to the ease of information content and flow. On the one hand, information is a message that contains meaning or content. Thus these media products convey a message designed to evoke certain emotions among the target audience, inducing support for the cause. Alternately, information is a medium in which communication takes place. The following analogy illustrates the difficulty in controlling the content and flow of extremist messaging.

These sophisticated media products are similar to music in lifecycle and appeal. Their propaganda value is non-perishable; time does not diminish their relevancy. When products hit the EMF, they are transmitted to other sites, emailed, or down-loaded and mass-produced for further dissemination. They can be quickly distributed or copied onto other media formats (CDs, VCDs, DVDs, cassettes, and thumb drives) for those without Internet access. Given their sensational nature, these products never lose their appeal, and can be played repetitively like a favorite song. For example, *Top 20*, produced by Ansar al-Sunnah, is a compilation video of attacks on US forces presented as a "greatest-hits" competition among insurgent brigades to provide the most spectacular attack footage. It is made with the express intention of encouraging rivalry among fighters. Because these products maintain their relevancy and appeal, the "shock and awe" value is preserved, thereby reducing the necessity of generating a constant supply of new products.

Once the *Top 20* hits the EMF, the flow of information through the multitude of dissemination points is impossible to interdict through purely technological methods. Dr. Muhammad Massari, the sponsor of the influential London-based website *Tajdeed,* notes:

I never touch the videos that are on my forums… Someone with Al Qaeda uploads them probably at Internet cafes to password-protected sites. Then they call a friend, say, in Australia or Brasilia, and say, 'Hi Johnny, your mom is traveling today." That is the code to download the video, it goes up and down like that a few times, with no trace until someone posts a link on my site.

Finally, and most significantly, DOD policy ignores the burgeoning demographic bubble of young Muslims and their susceptibility to the clarion call of "jihad" that these products advance. The youthful bent of the Muslim population represents a large recruitment pool for extremist organizations. The availability of the Internet in the global market ensures that these young people are more technology-oriented than the previous generations; and extremist media organizations are cognizant of its popularity and appeal.

Conclusion

While AQ copes with extreme losses to its leadership, debate over whether kinetic operations focused on "cutting off the head" leads to a diminution of the threat continues among pundits, politicians, and the military. This is because the same global information environment that challenges DOD efforts to combat extremist messaging simultaneously provides extremists opportunities to perpetuate a war of ideas on a global scale. Cyber-terrorism is more pragmatic and cost-effective than subordinating nation states through armed conflict. The shift from a war of violence in the physical world to a war of ideas in the information environment underscores the insidious nature of cyber-terrorism. Thus, maximizing our strategies to counteract this threat is critical to safeguarding long term peace and stability in the US and abroad.

Extending CYOP's mission fills an important gap in DOD's strategy that CNA and kinetic operations cannot counteract. CYOP provides a critical supplement to the limited technological approaches available in the CNA realm. CYOP is the appropriate response to the influence component of extremist Islamist messaging. However, CYOP success in this new role depends upon modifying relationships between the military and Internet authorities, as well as the legal framework, to avoid being hamstrung by national and political borders. Extremist messaging pervades the Internet, and DOD attempts to counteract it remain ineffective and haphazard without a comprehensive strategy including cyber psycholgical operations. To successfully counter extremist ideology, we must bring CYOP capabilities to the fight.